

---

# Mega Key Authentication Mechanism

*Release 7f6735f*

**Mega Limited, Auckland, New Zealand**  
**Guy Kloss <gk@mega.nz>**

30 October 2015

## CONTENTS

<b>1</b>	<b>Mega Key Authentication Mechanism</b>	<b>1</b>
1.1	Key Types . . . . .	1
1.2	Approaches for Key Authentication . . . . .	1
1.3	Key Trust . . . . .	2
<b>2</b>	<b>Key Authentication Tree</b>	<b>3</b>
2.1	Authentication of Identity Key (Ed25519) . . . . .	3
2.2	Authentication of Signed Public Keys . . . . .	3
2.3	Tracking of Consistency . . . . .	4
2.4	Key Fingerprinting . . . . .	4
<b>3</b>	<b>Key Authentication Workflow</b>	<b>5</b>
3.1	Loading of Unsigned Public Keys . . . . .	5
3.2	Loading of Signed Keys . . . . .	5
3.3	Own Key Initialisation . . . . .	6
<b>4</b>	<b>Future Work</b>	<b>8</b>
	<b>Bibliography</b>	<b>9</b>

## MEGA KEY AUTHENTICATION MECHANISM

For secure communication it is not just sufficient to use strong cryptography with good and strong keys, but to actually have the assurance, that the keys in use for it are authentic and from the contact one is expecting to communicate with. Without that, it is possible to be subject to impersonation or man-in-the-middle (MitM) attacks.

Mega meets this problem by providing a hierarchical authentication mechanism for contacts and their keys. To avoid any hassle when using multiple types of keys and key pairs for different purposes, the whole authentication mechanism is brought down to a single “identity key”.

### 1.1 Key Types

A number of key types are used on the Mega platform for different purposes.

**Signing/Identity Key (Ed25519).** For establishing the identity of a contact and transferring authenticity to data items via cryptographic signing EdDSA signatures are used with an Ed25519 elliptic curve signing key pair [Ed25519] (256 bit key strength).

**Sharing Key (RSA).** An RSA key pair (2048 bit key strength) is mainly used for sharing stored content with contacts. Additionally, it is used for establishing a voice/video connection using MEGAchat to avoid MitM attacks on the WebRTC channel between the peers.

**Chat Key (x25519).** For encrypting the sender (session) keys to recipients in MEGAchat, an elliptic curve Diffie-Hellman (ECDH) approach is used to enable only one self and the intended recipient access to the key. For this an x25519 key pair [x25519] (256 bit key strength) is used.

### 1.2 Approaches for Key Authentication

A number of approaches are commonly used for ensuring the authenticity of keys. The following are used within the Mega platform

**Key Comparison.** Keys are compared between contacts to ensure their authenticity. Such keys can be lengthy, therefore commonly a cryptographically secure hash function is used to compute a suitably sized “fingerprint”. For comparison of such keys/fingerprints it is essential to perform an “out of band” comparison with the contact, ideally directly in person with the assurance that no impersonator is involved. For people personally not known, other means of identification (e.g. a photo ID) may be used to assist the process of establishing the identity.

**Fingerprint Tracking.** Once a key has been encountered, its fingerprint is being tracked (stored privately in tamper-resistant data structure together with the contact’s ID). Should the case arise that in subsequent sessions a key’s fingerprint is changed, the user can be alarmed of this issue, and key authentication process can be initiated.

**Key Signing.** In case a contact’s authenticity of a signing key pair is given, any item requiring origin authenticity can be verified through a signature of that item. In this way public keys can be signed by the owner’s private signing key, and a contact can verify the signature using the trusted public key.

## 1.3 Key Trust

The Mega platform does already have some storage provisions for tracking a user's trust on individual keys. However this concept is not yet employed or exposed.

## KEY AUTHENTICATION TREE

We are distinguishing between *signed keys* and *unsigned keys*. Unsigned keys need to be authenticated directly, whereas signed keys are authenticated indirectly via a signature. The key used for signing is an unsigned key authenticated directly.

Authentication of all public keys is arranged in a flat hierarchy. The identity key is located at the top of the hierarchy (an unsigned key), which is then used to authenticate all other public keys (signed keys).

### 2.1 Authentication of Identity Key (Ed25519)

In order to protect oneself against bogus contacts, every key needs to be authenticated in some fashion. The main *identity* public key – an Ed25519 signing key – is authenticated directly by humans (unsigned key). This is commonly done by comparing a large enough portion of a hash value of the key, which has been obtained via a cryptographically secure hash function.

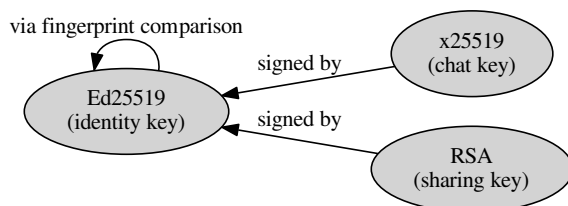
A manual fingerprint comparison is to be conducted through a reliable and trustworthy “out of band” channel. Ideally, this would be through a personal meeting in real life. At a minimum this could be done through a phone conversation with the contact, if one is able to ensure that the conversation partner on the phone is not an impostor (e.g. via familiar voice or information items that only that person may know). One needs to be aware that the authenticity is only as good as one is able to prevent any forgeries or impostors.

### 2.2 Authentication of Signed Public Keys

The identity key is a signing key usable for EdDSA cryptographic signatures. Therefore, all further public keys are signed cryptographically by it, and this resulting signature is made available to one’s contacts. With this, contacts can verify the authenticity of any additional public key, once they are sure that the identity key is authentic.

Even if authenticity of the identity key is not established, one can at least derive the knowledge that a set of keys is in itself consistent via verification of the signatures.

The following diagram shows the transitional authenticity relationships between public keys and the identity key.



## 2.3 Tracking of Consistency

Every public key of a key type is tracked in its own *authentication ring*. The authentication ring contains a key–value list, using a contact’s user handle as a key, and a record of the public key’s fingerprint, authentication method and trust level as a value.

### 2.3.1 “Seen” Keys

If no stronger form of authentication for a key is available, it will be tracked as “seen” for an authentication method. This allows the user client to raise an alarm in case the public key unexpectedly changes, whether it is due to an inconsistency (harmless, but hindering), or due to an attack attempt on the account of a contact.

### 2.3.2 Fingerprint Comparison of Keys

For the identity key we are offering the authentication via fingerprint comparison. The Mega client’s user interface exposes the identity key’s fingerprints as the “authenticity credentials” or “identity credentials” within the contact view. Ed25519 keys approved with this mechanism will be flagged with the “fingerprint comparison” authentication method. This is the most direct method of key authentication, but also the most bothersome to users. Therefore it is only employed for this particular key. See [Key Fingerprinting](#) for a description on how these fingerprints are obtained.

### 2.3.3 Signed Keys

The RSA and x25519 public keys are cryptographically signed using the Ed25519 identity key. These key signatures are stored as additional public user attributes. A contact can retrieve these signature values along with the public keys and the public Ed25519 key, and verify the integrity and authenticity of the signed keys. Such keys are flagged with the “signature verified” authentication method. This authentication method causes an almost imperceptible delay for a user on a particular key and is therefore employed where possible.

## 2.4 Key Fingerprinting

A key’s fingerprint is a shortened digest computed from a public key, that is sufficiently long enough as to be taken as a representation of a particular key that is unfeasible to be forged. This is commonly done by computing a large enough portion of a hash value of the key, which has been obtained via a cryptographically secure hash function. In Mega’s case, this is the slice of the most significant 160 bits of the SHA-256 hash function, represented in the user interface as 40 hexadecimal characters. This is the so called “fingerprint” of the public key.

Elliptic curve public keys (x25519 and Ed25519) are hashed directly in their byte (octet) representation in big-endian format. For RSA keys, the byte (octet) representations in big-endian format of the modulus ( $n = pq$ ) and the exponent ( $e$ ) are concatenated before being hashed.

## KEY AUTHENTICATION WORKFLOW

The main goal is to achieve the following for all keys: Obtain all keys in a way as to not encounter any undetected subversion, and to achieve maximum tracked authentication for all keys. As a secondary goal, we want to achieve the above under the minimum effort. This means, that we want to avoid any unnecessary API request/response round trips as possible.

Obviously caching is a complementary technique that may be employed for this purpose. However, it needs to be ensured that cache entries are not “stale” (outdated). But caching is beyond the scope of this document and shall not be further discussed here.

As a preliminary, for each key type the corresponding *authentication ring* needs to be loaded first. The authentication ring contains key fingerprints and authentication information for each contact the key has been loaded previously. Within the scope of this chapter, it is assumed that all authentication rings for all keys involved in a workflow are already loaded, i.e. for loading a chat key the x25519 authentication ring is loaded, as well as possibly the Ed25519 authentication ring when verification of the signature is required.

See Fig. *Key loading workflow* for a visual overview of the key loading procedure outlined below.

### 3.1 Loading of Unsigned Public Keys

Loading unsigned public keys (such as the Ed25519 identity key) is very simple and straight forward. The contact’s public key is loaded, and its fingerprint is obtained. If a record for that particular contact’s identity key is already available in the authentication ring, the fingerprints are compared. An error dialogue corresponding to this condition is raised for the case of mismatching fingerprints. If a key’s fingerprint is not tracked, yet, the fingerprint for the contact is added to a record in the key’s authentication ring (with the authentication method set to “seen”).

### 3.2 Loading of Signed Keys

Loading of signed sub-keys (x25519 and RSA) is more involved, depending on the availability of signatures (older clients may not have stored key signatures, yet).

#### 3.2.1 Loading Public Keys without Signature

In the case of the absence of signatures, the key loading mechanism is similar to the loading of the identity key (see *Loading of Unsigned Public Keys*). The public key is loaded, and the fingerprint is compared to that in the corresponding authentication ring. In case of mismatches an error dialog is raised, in case of a missing entry it is added as a tracked “seen” key.

#### 3.2.2 Loading Public Keys with Signature

Firstly the public key is loaded, and its fingerprint is obtained through hashing. If it is already tracked in the authentication ring, the common fingerprint comparison is performed. If this comparison is failing, the key is not tracked, or it is tracked as only having been seen, we need to go a step further. The key’s signature as well as

the contact's public identity key are loaded. Subsequent loading of the public identity key obviously involves that particular key loading mechanism (see *Loading of Unsigned Public Keys*). The public key's signature is verified. Upon positive validation the public key is tracked as "signature verified". This may mean that a newly created signature of a public key may "upgrade" the authentication status of a key from "seen" to "signature verified". If the verification fails, an error dialog is raised to indicate this condition to the user.

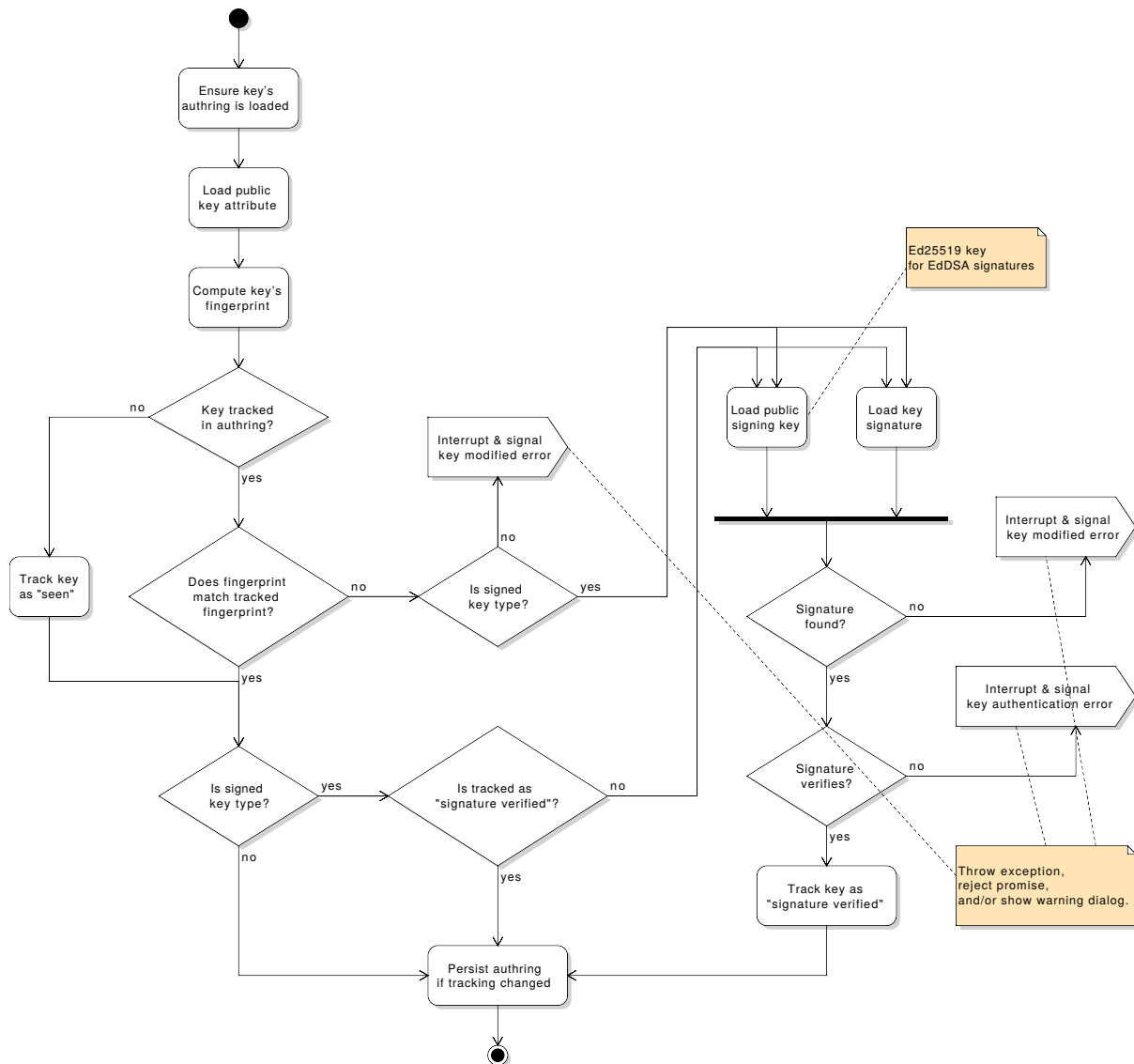


Fig. 3.1: Key loading workflow

Activity diagram for loading other contacts' public keys along with key authentication tracking.

### 3.3 Own Key Initialisation

When loading one's own keys for operation, the client is to perform sanity checks, and generate potentially missing keys. There have been cases due to bugs and race conditions where some public/private key pairs were inconsistent with each other, and some clients do not support all key types, yet. Therefore a proper procedure for initialisation and loading is outlined here (see Fig. *Key initialisation workflow*).



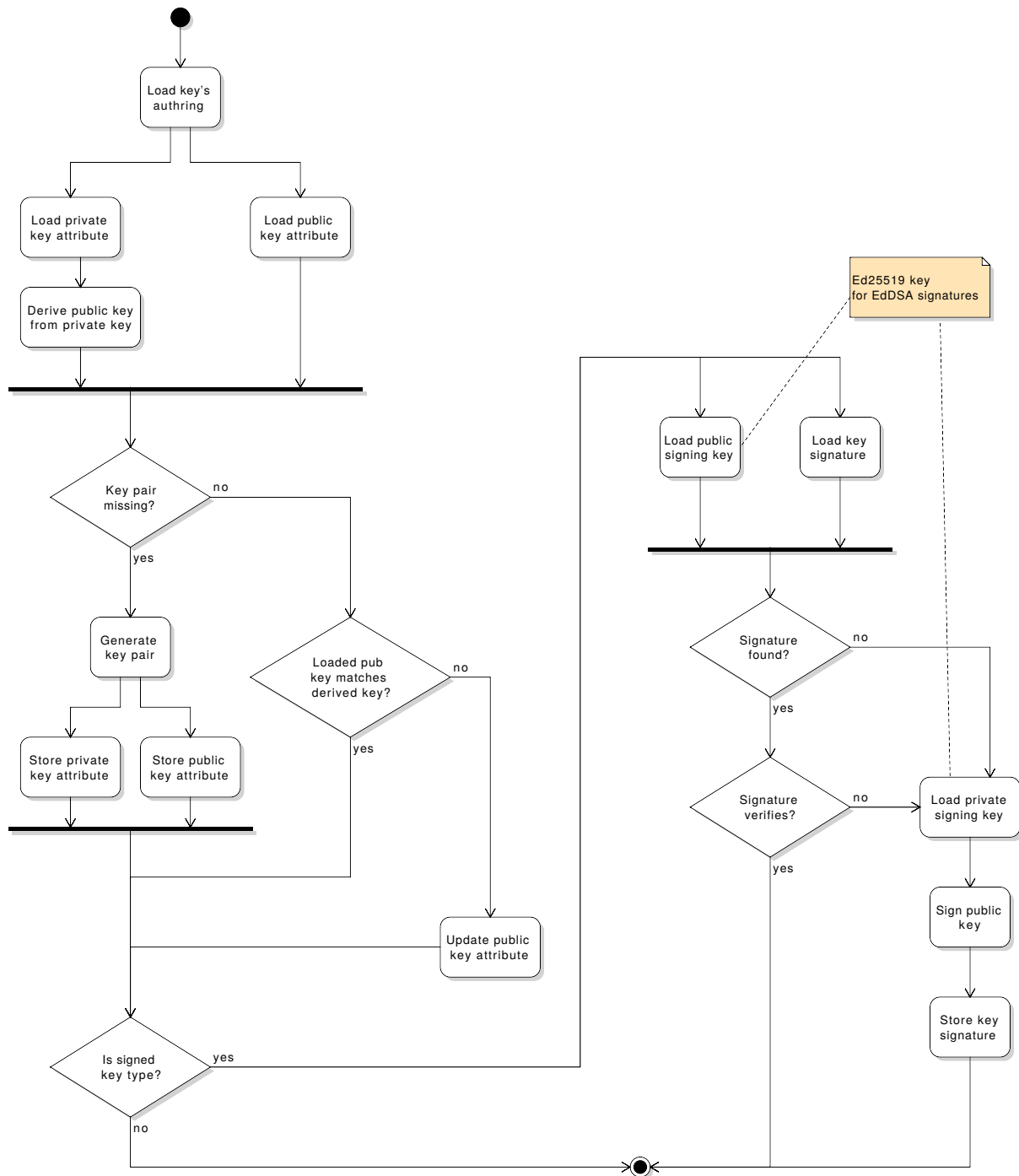


Fig. 3.2: Key initialisation workflow

Activity diagram for the initialisation and loading of one's own key pairs, along with resolution of missing attributes or inconsistencies.

## FUTURE WORK

**Integration of further keys and key types.** Future development may demand other key types beyond the currently available ones. This could for example be an OpenPGP key pair.

**Enabling key versioning and rotation.** Keys and key pairs may be considered to be “burnt” (e.g. over used, compromised, not considered strong enough) and are in need of being upgraded by the user. In these cases old keys need to remain available (e.g. for old/legacy shares), and keys need to be explicitly referenced by some version identifier. Additionally, the problem of transitive key authentication needs to be solved.

**Key trust.** As mentioned initially, we do not expose any mechanisms for trusting specific keys differently, or for altering such trust levels. The key tracking mechanism does already provide a limited attribute for this, but it is not used, yet.

**Web of Trust.** From the current vantage point a *Web of Trust* (WoT) is an interesting idea. However, it is mostly not exercised “in the wild” (e.g. with OpenPGP). We are not going into the trouble of discussing any issues further here, but it seems unlikely that a WoT approach will be implemented on top of the Mega platform.

## BIBLIOGRAPHY

[Ed25519] <http://ed25519.cr.yp.to/>

[x25519] <http://cr.yp.to/ecdh.html>